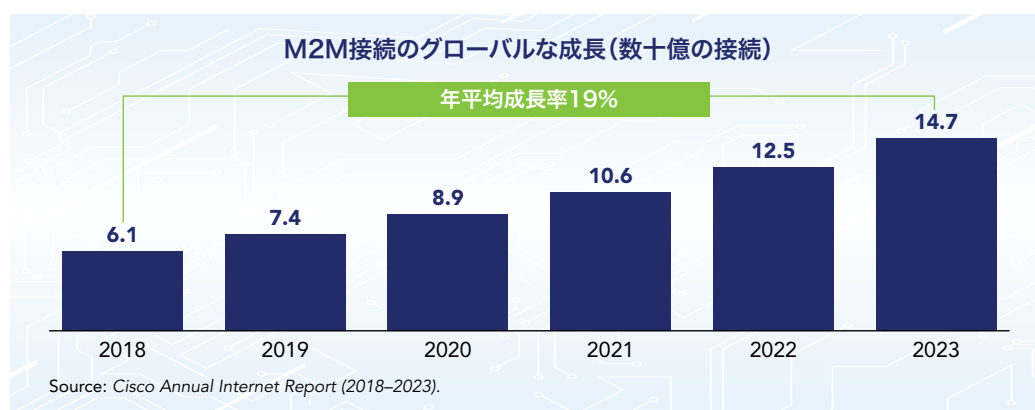
安全で信頼できるIoT（モノのインターネット）構築のためのBSAのポリシー原則

インターネットの常に進化する性質によって、デバイス、アプリケーション、サービス間の通信に新たな可能性が生まれ、これが私たちの物理的環境、仕事、社会との日常の関わりまでも変革させています。モノのインターネット（IoT）は、世界をより良いものに変える大きな可能性を秘めています。IoTがインターネットや世界経済に今後与える影響は多大なものであり、IoTデバイスとそのさまざまなアプリケーションでの使用の数は爆発的な増加が予測されます。世界的に見ると、IoTを含むマシンツーマシン（M2M）接続は、2018年の61億から比べて今後数年で2倍以上になり、2023年までには147億に達するでしょう。[1]

世界的に見ると、IoTを含むマシンツーマシン（M2M）接続は、2018年の61億から比べて今後数年で2倍以上になり、2023年までには147億に達するでしょう。

Source: *Cisco Annual Internet Report (2018–2023).*

数十億ものIoTデバイス、アプリケーション、サービスがすでに使用されており、日々ネットワーク上に増え続けています。そして新しいデバイスが登場するたびに、悪意ある行為者がデジタルエコシステムを破壊する機会が拡大するのです。ある試算では、2019年前半のIoTデバイスに対するサイバー攻撃は、2018年後半に比べて300%増加したと述べています。[2] IoTの成長に伴い、IoTセキュリティは最重要事項となりました。セキュリティ保護が不十分なIoTデバイスとサービスは、サイバー攻撃の入り口となってしまい、機密データを危険にさらし、個々のユーザーの安全を脅かします。脆弱なセキュリティの

---

[1] シスコ、*Cisco Annual Internet Report (2018–2023)*、https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.pdf

[2] F-Secure、*Attack Landscape H1 2019*、https://blog-assets.f-secure.com/wp-content/uploads/2019/09/12093807/2019_attack_landscape_report.pdf、以下も参照：Zak Doffman著、「Cyberattacks On IOT Devices Surge 300% In 2019, 'Measured In Billions', Report Claims」、フォーブス（2019年9月14日）、https://www.forbes.com/sites/zakdoffman/2019/09/14/dangerous-cyberattacks-on-iot-devices-up-300-in-2019-now-rampant-report-claims/#220ecd435892

IoTデバイスのネットワークを利用した、インフラストラクチャやその他のユーザーへのサイバー攻撃は、医療や公益事業などの不可欠なサービスの提供に影響を与え、人々のセキュリティやプライバシーを危険にさらし、世界中でインターネットの耐障害性を脅かす可能性があります。

これらの難題は、政府とテクノロジー業界が力を合わせてIoTのセキュリティ強化を図っていく十分な理由となります。政策立案者は、課題を検討し、解決策を特定する余地のある措置を取る必要があります。

BSA会員企業は、世界のソフトウェア業界で信頼されるリーダーとして、IoTセキュリティの進歩を含めIoTイノベーションの最前線に立っています。政府のIoTセキュリティ政策に関し、BSAは、責任あるリスクベースのアプローチを含む、IoTの信頼構築のための一連の原則を支持します。

IoTセキュリティ政策は、IoTエコシステムの多様性と複雑さに対応する

IoTの定義として広く認められたものはありませんが、一般的には、センサー、ソフトウェア、その他のテクノロジーが組み込まれた物理的なオブジェクト(「モノ」)のネットワークを指し、インターネット経由で他のデバイスやシステムとデータを接続したり交換したりすることを目的としています。

IoTシステムには、一般的にセンサーやアクチュエーター、データプロセッサー、ユーザーインターフェースなどのデバイス要素と、ゲートウェイやクラウドインフラストラクチャーなどのネットワーク要素が含まれます。

主要な要素

IoTデバイス：IoTデバイスは、インターネットに接続することができ、また通常はインターネットに接続されており、データを収集、送信、または受信できるコンピューター処理機能を備えています。IoTデバイスには、ユーザーインターフェース、データプロセッサー、複数のセンサーが組み込まれている場合があります。たとえば、IoTデバイスにはGPS、加速度センサー、カメラセンサーを搭載できます。デバイスは、プログラマブルロジックコントローラ（PLC）などの複雑なシステムの場合もあれば、オペレーティングシステムを持たないような非常に単純な場合もあります。

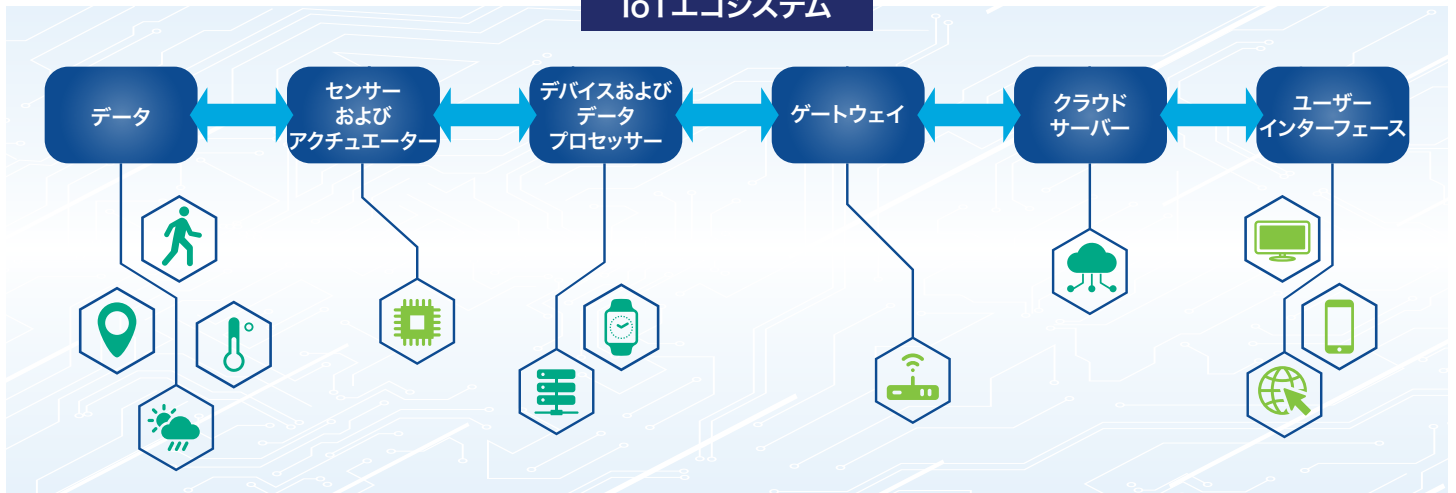
» **センサーおよびアクチュエーター：**センサーは周囲の環境からデータを収集します。この収集されたデータは、単純な温度監視から複雑なビデオフィードまで、その煩雑性はさまざまです。アクチュエーターはセンサーから情報を受信し、それを物理的な動作に変換します。たとえば、電動モータや油圧システムに作動するよう指示します。

» **データプロセッサー：**データプロセッサーとは、データを有用な情報に変換するための操作を実行するコンポーネントを指します。これらの情報は解釈され、分析に使用できます。データ処理機能は、圧力測定値が許容範囲内であることの確認などの単純なものから、コンピュータビジョンを使用してビデオ内のオブジェクトを識別するなどの複雑なものまで多岐にわたります。

» **ユーザーインタフェース：**ユーザーインターフェースは、画面、ページ、ボタン、フォーム、アイコン、テキストなど、エンドユーザーがIoTシステムとやり取りするための機能で構成されています。ユーザーインターフェースは、IoTデバイスのリモート管理に使用される製品、ポータルまたはアプリケーションとユーザーとのやり取り、すなわちユーザーエクスペリエンスと密接に関連しています。

ネットワーク：ネットワークでは、IoTデバイスによって収集されたデータをクラウドインフラストラクチャに転送できます。IoTデバイスは、携帯電話ネットワーク、衛星ネットワーク、Wi-Fi、Li-Fi、Bluetoothなど、さまざまな通信および転送媒体を介してクラウドに接続できます。新しいエッジコンピューティング機能を備えた5Gネットワークは、IoTデバイスの使用と管理に無数の新たな可能性を生み出します。ネットワーク、ゲートウェイ、クラウドインフラストラクチャに関連するのは、IoTエコシステムの他の重要なコンポーネントです。

» **ゲートウェイ：**ゲートウェイは、IoTデバイスと接続先ネットワーク間のデータトラフィックを管理します。ハードウェアやソフトウェアの要素が含まれている場合があります。たとえば、家庭使用環境では、ルーターがホームWi-Fiネットワークとインターネットサービスプロバイダーの間のゲートウェイとして機能することがよくあります。ゲートウェイは、数千台のセンサーから収集されたデータをローカルで前処理してから次のステージに送信するように設定できます。ゲートウェイのもう一つの機能として、異なるネットワークプロトコルを変換し、接続されたデバイスとセンサーが相互運用可能であるようにします。また、ゲートウェイは、高階の暗号化技術を使用して、ネットワークおよび送信データに対して一定レベルのセキュリティを提供することもできます。デバイスとクラウドの中間層として機能し、悪意のある攻撃や不正アクセスからシステムを保護します。

» **クラウドインフラストラクチャ：**クラウドインフラストラクチャとは、大量のデータを効率的に処理するために最適化された分散コンピューティングおよびデータベース管理システムを指します。クラウドサーバーは、大量のデータをリアルタイムで収集、処理、管理、保存するツールを提供し、多くのセンサー、デバイス、ゲートウェイ、プロトコルからの入力を統合します。また、カスタマイズされたセキュリティ制御やその他のルールを特定のシステムグループに適用できる仮想環境やコンテナ化された環境を作成し、IoTデバイス管理用の強力なツールを作成できます。

これらのさまざまなコンポーネントは、IoTがモノリスではなく、さまざまなデバイス、通信ネットワーク、インターフェース、そして人を含む複雑なシステムであることを示しています。多くのサードパーティを含む複雑なサプライチェーンでは、セキュリティ評価が困難になり、システムをさまざまな関係者やシステムの各部と連携して総合的に保護する必要があります。さらに、IoTには、クラウドサービスや通信ネットワークなど、他の政策の対象となる要素も含まれます。

政府は、IoTエコシステムの複雑さと多様性を総合的に考慮し、システムの各部分が果たす役割と、それらの部分がどのように相互作用するかを認識し、そのような複雑さに対応できて技術的中立性が保たれている柔軟な政策を策定する必要があります。さらに、IoTセキュリティ政策は、クラウドや5Gセキュリティなど、IoTエコシステムのさまざまな要素に影響を与えるセキュリティ政策と一致し、適合するものでなければなりません。

伝わりやすく、使いやすいIoTセキュリティ政策により、消費者はデバイスのセキュリティ・プラクティスや機能を簡単に理解できます。

IoTセキュリティ政策は、重要な概念と要件を明確に定義する

政府機関がIoTセキュリティ政策を策定する際、政策立案者は、技術的な定義とセキュリティ要件を明確に定義する必要があります。消費者、産業界、その他の利害関係者に政策の範囲と意図を明確に伝達し、断片化された定義を作らないようにするには、「IoT」や「IoTデバイス」などの主要な用語について、国際的な合意に基づく広く採用された標準に従った明確で理解しやすい定義を設けることが不可欠です。同様に、IoTセキュリティ政策内のセキュリティ要件を明確に定義する必要があります。政策立案者が特定のセキュリティ対策を要件に設定するのなら、これらの政策によって、（国際標準化機構や国際電気標準会議などにおいて）適切かつ合理的とされる機能およびプロトコルを概説する確立された国際標準を製造業者が採用するように、適切なインセンティブを与える必要があります。また、現在の機能および慣行はすぐに時代遅れになるかもしれないので、体系化するのは避けるべきです。伝わりやすく、使いやすいIoTセキュリティ政策により、消費者はデバイスのセキュリティ・プラクティスや機能を簡単に理解でき、IoTメーカーやベンダーがセキュリティの優先事項に効率的に対処できるようになります。多くの場合、IoTセキュリティ政策の主な定義と要件は過度に広範であるか、大幅に省略されているため、消費者と企業を混乱させてしまいます。

各国政府は、IoTセキュリティに関連する主要な概念と要件を、可能な限り国際標準に沿って明確に定義する必要があります。

「IoTデバイス」の定義

政策立案者は、どのデバイスが対象になるかを、可能な限り具体的かつ明確にIoTセキュリティ政策で定義する必要があります。一般的に、IoTセキュリティ政策では、次のような「IoTデバイス」の定義を使用すべきです。

» ネットワークに接続するように設計されたデバイスで、データの収集、送信、または受信に必要なコンピュータ処理機能を含む。

» エンドユーザーが使用できる完成品で、他の製品に組み込まれたり統合されたりすることなく、目的の機能に使用でき、コンポーネントではない[一部のIoTデバイスは大規模なシステム内で使用されることがあり、併せて複合IoTデバイスを構成する場合がある(接続カメラや接続デジタルディスプレイなど、多くのIoTデバイスが接続されている「スマートバス」を想定)が、このような複合IoTデバイスであっても、個々でIoTデバイスと見なすためには、組み込まれたデバイスは個別に機能する必要がある]。

» IoTデバイスは、他のコンポーネント、デバイス、システムを含む幅広いエコシステムに接続するように設計されていることを認識している

» パーソナル・コンピューティング・システム、スマートモバイル通信デバイス、メインフレーム・コンピューティング・システムなどの一般的なコンピューティング・デバイスは含まない。

革新的なアプローチとして、IoTデバイスを保護する方法はデバイスベースではなく技術や方法論に依存するようになってきています。

IoTセキュリティ政策は、デバイスだけでなく、IoTエコシステム全体を保護する

望ましいセキュリティの成果を得るためのリスクベースのアプローチは、運用環境に応じてさまざまです。革新的なアプローチとして、IoTデバイスを保護する方法はデバイスベースではなく技術や方法論に依存するようになってきています。場合によっては、これらのアプローチがデバイス中心のセキュリティ対策の代わりになるかもしれません。

IoTセキュリティ・ガイダンスの開発に向けた多くの取り組みは、デバイスの特性に限定的に焦点を当てています。エコシステムの観点を考慮したセキュリティのアプローチでは、IoTデバイスのセキュリティベストプラクティスは確かに重要であり、またIoTシステムのすべての要素をセキュリティで保護することも同程度に重要であると示唆しています。さらにいえば、セキュリティ対策は足並みを揃える必要があるのです。政策立案者は、ベンダーや顧客がデバイス外のセキュリティ対策に革新をもたらし、これを適用する能力が、デバイス中心のセキュリティ政策によって損なわれないようにする必要があります。たとえば、IoTデバイスのパスワード要件を設定することは、セキュリティとユーザーエクスペリエンスの両方を向上させるシングルサインオンID管理テクノロジーの妨げとなるため、これらは政策では回避されるべきです。

同様に、多くのセキュリティ専門家は、IoTデバイスすべてが安全なパッチやアップデートを受信できるようにすべきだと主張しています。この機能により、ベンダーは、発見された脆弱性を緩和するなど、デバイスの保守性を向上させることができますが、デバイスのコスト、市場投入までの時間、複雑さの面での妥協を招く可能性があります。ただし、そのような機能の実装を妨げる可能性のある使用要件によって、デバイスの性能が制限される場合があります。新たな選択肢の1つとして、カスタマイズされたクラウド環境の構築が挙げられます。管理者は、環境内で管理されているデバイスに合わせてカスタマイズされたセキュリティルールを適用できます。たとえば、デバイス自体に新しいソフトウェアをインストールすることなく、特定のデバイスの脆弱性を緩和する「仮想パッチ」を適用できます。

もう1つの例として、「Manufacturer's Usage Description」(MUD)があります。MUDは、デバイスが重要な情報をルーターに通信して、安全な管理を可能にするためのプロトコルです。この場合、デバイス(デバイスのデータ、通信プロトコル、および使用パターンに関する情報を記載するソフトウェアタグを含む)は、ルーターと連携して動作します。ルーターは、セキュリティルールを適用し、デバイスに関する公開情報に基づいて異常な動作を識別します。

政府は、エコシステム内のすべての要素(IoTテクノロジー全体に導入されたソフトウェア、ファームウェア、ハードウェアなど)を考慮し、高度なネットワークベースのセキュリティ対策の開発と適用を妨げるデバイス中心の政策を回避することで、信頼と安全に対するリスクベースのアプローチを推進する必要があります。

IoTセキュリティ政策は、コンシューマー向けIoTと産業用IoT(IIoT)を区別する

一般的に、ウェアラブル端末、スマートホーム・アプリケーション、個人の健康管理デバイスなどのコンシューマー向けIoTソリューションは、個々のユーザーや家族をターゲットにしています。管理対象外の環境や限定的なネットワーク管理が行われている環境で使用される傾向があり、最小限のセキュリティサービスを使用するか、まったく使用しない場合もあります。これらのデバイスは長年にわたって使用可能ですが、新世代のテクノロジーの登場により、急速に新しいバージョンに置き換えられる傾向があります。

IIoTとは、産業分野およびアプリケーションにおけるIoTの拡張と使用を指します。IIoTは、M2M通信、ビッグデータ、機械学習に重点を置いており、大規模工場や製造工場などの生産性と効率の大幅な向上を求める既存のオートメーション化された産業システムを対象としています。その他のIIoTテクノロジーの例としては、コネクテッドHVACシステム、スマートグリッドテクノロジー、手術室で相互接続システムを利用した医療機器などがあります。さらに、一般的に、商用または法人向けテクノロジーは、コンシューマー向けIoTではなく産業IoT関連の政策によって対処されるべきです。法人向けIoTとは、商業オフィスビル、スーパーマーケット、ホテル、医療施設、小売店などのアプリケーションを指します。法人向けおよび産業用IoTテクノロジーは、多くの場合、高度なネットワーク保護を使用して十分に管理された環境で機能します。さらに、重要なインフラ分野に導入されているIIoTについては、国家安全、公衆衛生または安全、経済活力、あるいはその組み合わせに対するこれらのアプリケーションの重要性から、個別に検討することが必要になる場合があります。

法人向けおよび産業用IoTテクノロジーは、多くの場合高度なネットワーク保護を使用して十分に管理された環境で機能します。

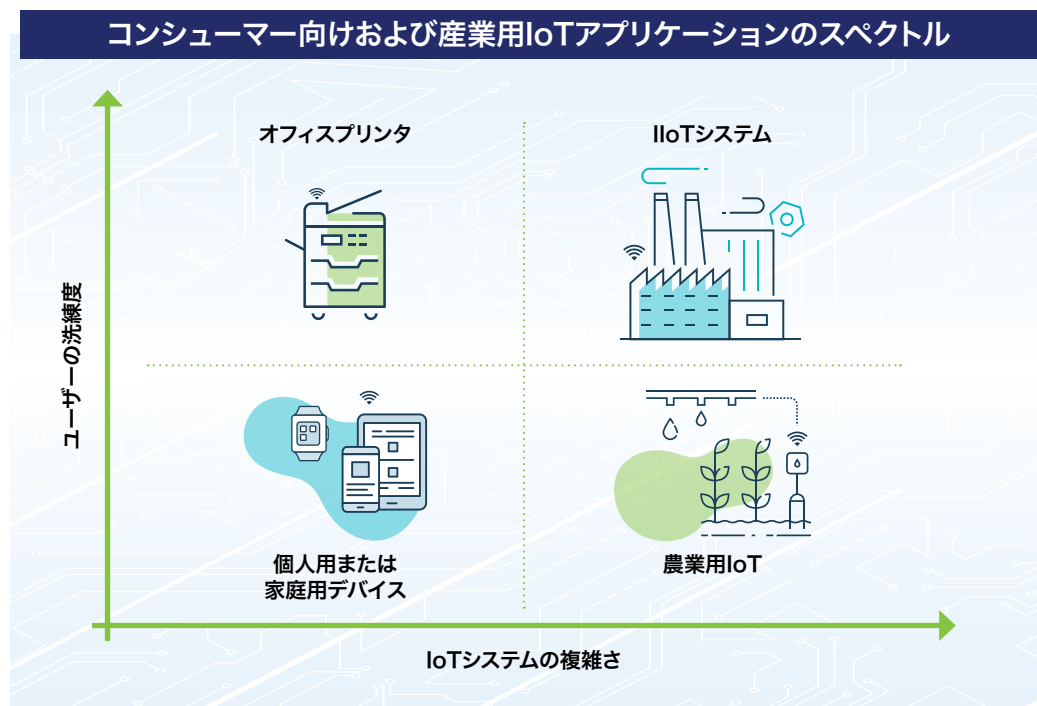
コンシューマー向けIoTおよびIIoTソリューションは、ネットワーク環境、リスクレベル、サポートライフサイクル、複雑性の点で異なります。

- **ネットワーク環境:**コンシューマー向けIoTは、一般の家庭やオフィスで使用されています。通常、このようなユーザーは、テクノロジーを導入する前にサイバーセキュリティトレーニングを受けることはありません。さらに、家庭用ルーターや、コンシューマー向けIoTが接続するネットワークなどの機器は、専門的に管理されることはほとんどありません。一方、IIoTソリューションは通常、社内のサイバー専門家によって導入および保守されます。IIoTが接続するネットワークも、ほとんどの場合、複雑なネットワーク保護を導入しているセキュリティ専門家によって管理されます。IIoTは多くの場合、重要な産業機能を支えているためです。
- **リスク:**コンシューマー向けIoTとIIoTは、これらのテクノロジーが著しくさまざまな環境に適用されるため、さまざまなセキュリティ上のリスクをもたらします。一般的なコンシューマー向けIoTのリスクには、ボットネット、ランサムウェア、ID窃盗などがあります。これらのソリューションは、家庭用機器やネットワーク上で一般的な人によって頻繁に使用されるからです。IIoTは、製造工場や発電所などの

重要なインフラ環境に導入されることが多いため、IIoTセキュリティインシデントは、機器の故障、重要なデータの損失、ビジネスおよび社会的な混乱、または怪我や生命の損失までもが発生する危険性があります。IIoTシステムの複雑さも、悪意ある攻撃者にとっては攻撃しやすい対象となります。

» **サポートライフサイクル：**コンシューマー向けIoTのテクニカルセキュリティサポートは、IIoTと比べ比較的限られています。一般コンシューマー向けIoTソリューションでは、多くの場合、実用性中心のセキュリティ対策を実装して、ユーザーエクスペリエンスと消費者が製品を使用する際の利便性を優先します。逆に、IIoTソリューションでは、通常高度で堅牢なセキュリティ対策とプロトコルが使用されます。コンシューマー向けIoTベンダーはIoTデバイスにサービスを提供していますが、一般消費者は法人管理ツールにアクセスできず、数年ごとにデバイスを交換することがあります。IIoTのデバイスでは、多くの場合、セキュリティに長期的な投資が必要になります。これには、社内および現場のサービス技術者によるメンテナンスが含まれ、産業用システムで必要とされるパフォーマンスレベルを維持することが含まれます。また、IIoTセンサーは、地表下や海外にある石油・ガス施設など、物理的にアクセスが困難なリモートインフラでのパラメーターを測定するために設置されることがよくあります。内部管理機能には、センサーの交換、ファームウェアのアップグレード、ゲートウェイとサーバ構成の管理などがあります。

» **複雑さ：**コンシューマ向けIoT製品は、IIoTソリューションと比較して、統合を必要としません。IIoTシステムは、広範なレガシー運用技術（OT）を使用する複雑な環境に適用されます。OTとは、ヒューマンマシンインターフェース（HMI）、監視制御およびデータ収集（SCADA）システム、分散制御システム（DCS）、プログラマブル・ロジック・コントローラ（PLC）などの運用プロセスおよび産業制御システム（ICS）のネットワーキングを指します。IIoTソリューションは、これらの既存の製造システムと確実に統合する必要があります。つまり、これらの環境でのパッチ管理やその他の主要なセキュリティ対策は、はるかに複雑化します。

コンシューマー向けIoTとIIoTは、これらのテクノロジーが著しくさまざまな環境に適用されるため、さまざまなセキュリティ上のリスクをもたらします。

政策立案者は、コンシューマー向けIoTとIIoTのこれらの重要な違いを考慮し、リスクに基づいてIoTのセキュリティガイダンスと取り組みを優先順位付けする必要があります。

政府は、すべてに適合する単一のアプローチを追求するのではなく、コンシューマー向けIoTおよびIIoTテクノロジーによってもたらされるさまざまなリスクに対処する必要があります。コンシューマーデバイスの政策では、デバイス内でのセキュリティの構築を優先的に行う必要があります。これは、消費者が安全で管理された環境を構築するためのリソースを持っていない可能性があるためです。一方、産業用ユーザーには、独自の複雑な運用環境に合わせてセキュリティ対策を調整できる柔軟性が必要でしょう。

IoTセキュリティ政策は、業界のベストプラクティスに基づいて構築される

多くのテクノロジー企業は、セキュリティ・イノベーションの最前線に立ち、IoTセキュリティのためのベストプラクティスを開発してきた数十年に及ぶ経験を持っています。多くのBSA会員企業も、セキュリティの点では競合しています。しかし、IoTテクノロジーの開発と導入の場面では、セキュリティに関する十分な情報に基づいた意思決定を行うための知識と専門知識をすべての企業が持っているわけではありません。政府は、セキュリティ・バイ・デザインの原則から、分野固有の製品開発およびリスク評価ガイドまで、さまざまなベストプラクティスを推進することで、より優れたセキュリティ結果を実現できます。

特に、多くのベストプラクティスでは、セキュリティに対処するためのリスクベースのアプローチが採用されています。リスクベースのフレームワークは、政策立案者、デバイスメーカー、およびユーザーが、使用されている特定の状況で特定のデバイスに影響を与える可能性が最も高いリスクを理解し、対処するのに役立ちます。リスクベースのフレームワークには、ユーザーのリスク（IDの盗難や評判の低下など）、サイバーセキュリティリスク（主要機能の中断など）や物理的リスク（物理システムの損傷または破壊）を含む、影響を受けるシステムまたは資産のリスク、および、より広範なエコシステム（ボットネットによる乗っ取りや経済的な混乱など）へのリスクについての分析を組み込む必要があります。リスクベースのフレームワークは、IoTセキュリティに対する政策アプローチの中心となるべきです。

業界の合意形成の取り組みにより、広く受け入れられるIoTセキュリティガイダンスの開発が大幅に進展しています。たとえば、「BSA Framework for Secure Software（安全なソフトウェアのBSAフレームワーク）」[3]は、主要なエンタープライズソフトウェア企業のベストプラクティスを活用して、ソフトウェア開発組織、その顧客、および政策立案者に、ソフトウェアのライフサイクル全体のセキュリティを評価し、奨励するためのガイダンスを提供しています。このソフトウェアには、IoTソリューションを強化するものも含まれます。さらに、C2 Consensus on IoT Security Capabilities[4]では、20の主要なサイバーセキュリティおよびテクノロジー組織のグループが集まり、IoTデバイスがセキュリティに対する市場の期待を満たし、世界中で政策を調和させるために必要な重要なセキュリティ機能に関するガイダンスをIoTデバイスメーカーに提供します。政策立案者は、業界から開発されたこれらガイドを参照して、断片化を軽減し、IoTエコシステムのさまざまな業界分野や部門の間で良好なサイバー衛生を促進する、より効果的なIoTセキュリティ政策の情報を発信することが期待されます。

政府のIoTセキュリティ政策は、業界を率いるリーダーたちの専門知識を取り入れ、広く受け入れられかつ業界で開発されたリスクベースのIoTセキュリティのベストプラクティスを取り入れることで、IoT市場全体のセキュリティを強化する必要があります。

[3] BSA Framework for Secure Software、https://www.bsa.org/reports/bsa-framework-for-secure-software

[4] The C2 Consensus on IoT Security Baseline Capabilities、https://securingdigitaleconomy.org/projects/c2-consensus/

IoTセキュリティ政策により、IoTライフサイクル全体を通じたセキュリティを奨励する

セキュリティは、開発から終了まで、IoTソリューションのライフサイクルのあらゆる段階に組み込む必要があります。長期的なセキュリティには、安全な開発およびセキュリティ・バイ・デザインのアプローチに加え、ソフトウェア、ハードウェア、およびファームウェアコンポーネントを保守し、実装後の脆弱性に対処するためのライフサイクル管理アプローチが必要です。脆弱性は、多くの場合、独立したセキュリティ専門家や調査コミュニティの人によって特定され、ベンダーに報告されます。製品のメンテナンスと脆弱性管理に対する総合的なアプローチの一環として、ベンダーは、このようなサードパーティのレポートを受信して対処するための明確な手順を確立する必要があります。セキュリティ専門家は、この重要なニーズに対応するために、脆弱性協調開示（CVD）プログラム[5]に関するガイダンスと標準を作成しています。これらのプログラムはすべて、国際的に認められたISO/IEC 29147および30111規格に準拠している必要があります。

IoTライフサイクル全体を通じてセキュリティの成果を向上させるために、政策立案者は、（1）国際的に認められた規格（特にISO/IEC 29147および30111）に適合し、（2）人工的な緩和スケジュールなどの非生産的な要件を回避し、さらに、（3）IoTソリューションのライフサイクル全体にわたって脆弱性管理に対する包括的なアプローチを反映するCVDプロセスを、自発的に確立するよう企業を奨励する必要があります。

エンドオブライフ（EOL）・ポリシーも、製品のメンテナンスと脆弱性管理に対する包括的なアプローチには欠かせない一部です。エンドオブライフ（EOL）とは、エンドユーザーに提供された製品が（ベンダーの観点から）耐用年数の終わりにあると判断され、ベンダーが製品のマーケティング、販売、または維持を停止する日付を指します。サポートされていないIoT製品やサービスを継続的に使用したり、サポートを突然終了したりすると、深刻な結果を招く可能性があります。特に、最新でないIoT製品はハッカーやバグに対して脆弱であり、これらのIoTテクノロジーに接続されている他のシステムに脆弱性が生じる可能性が高いためです。

IoTライフサイクル全体を通じてセキュリティに包括的に対応するために、政策立案者は、（1）IoT製品またはサービスの耐用年数終了日および耐用年数終了日に関する最新の予測に基づき常に更新され、（2）変化する状況に対応できる柔軟性を備えた、自発的なエンドオブライフ（EOL）・ポリシーの確立を企業に奨励する必要があります。

政府は、IoTライフサイクル全体を通じたセキュリティを促進するために、CVDプロセスとエンドオブライフ（EOL）・ポリシーを自発的に確立するよう企業を奨励する必要があります。

長期的なセキュリティには、安全な開発およびセキュリティ・バイ・デザインのアプローチに加え、ソフトウェア、ハードウェア、およびファームウェアコンポーネントを保守し、実装後の脆弱性に対処するためのライフサイクル管理アプローチが必要です。

IoTセキュリティ政策は、マルチステークホルダー・プロセスを採用する

IoTは急速に発展する環境の中にあり、そのテクノロジーは多くの業界や用途に広がっているため、課題の多い政策分野です。IoT市場が急速に進化するにつれ、BSA会員企業を含む業界の多くは、IoT分野における革新的で責任あるセキュリティ手法とプラクティスの開発の最前線に立っています。政府は、オープンで透明性が高く、合意に基づく複数の利害関係者（マルチステークホルダー）によるプロセスを通じてIoTセキュリティ政策を策定することで、業界が開発した専門知識を学び、これを取り入れることができます。さらに、複数の利害関係者によるプロセスにより、消費者グループや学者など、IoTに重点を置いた人々の視点から学習し、それを取り入れることができます。

[5] ソフトウェア脆弱性開示について、詳細は、BSA Guiding Principles for Coordinated Vulnerability Disclosure、https://www.bsa.org/files/policy-filings/2019globalbsacoordinatedvulnerabilitydisclosure.pdfを参照。ハードウェア脆弱性開示については、Center for Cybersecurity Policy and Law、「Improving Hardware Component Vulnerability Disclosure」https://centerforcybersecuritypolicy.org/improving-hardware-component-vulnerability-disclosureを参照。

また、このプロセスにより、IoT製品を開発、販売、使用するさまざまなメーカー、ベンダー、消費者をまとめることもできます。IoTテクノロジーは多くの業界に広がっていますが、IoTソリューションを開発して使用するすべての企業は、セキュリティを優先して、IoTシステム全体をサイバー脅威から保護すべきです。IoTセキュリティへの協働的なアプローチに参加することで、参加者は、ベストプラクティスと教訓を共有し、セキュリティ対話を促進し、時間の経過とともに変化する脅威に適応して進化できる柔軟な共有セキュリティソリューションを開発する機会を得ます。効果的かつ適切なIoTセキュリティ政策を策定するには、幅広い利害関係者の専門知識と関与を活用した協働的なアプローチが必要です。

政府は、複数の利害関係者による活動や作業グループを始動、統率、サポートし、業界やその他の関係者と協力して進化する脅威を理解し、既存の、合意に基づくガイドラインをもとに、IoTセキュリティのベストプラクティスを開発する必要があります。

IoTセキュリティ政策は、国家および国際的な政策の調和を図る

国家レベル（オーストラリア[6]、欧州連合[7]、日本[8]、シンガポール[9]、英国[10]）、州レベルまたは地方レベル（米国カリフォルニア州[11]およびオレゴン州[12]）を含む多くの政府が、IoTセキュリティに対応するための取り組みを行ってきました。より多くの政府がこの差し迫った問題に適切に焦点を当てるようになると、政策間で断片化のリスクが増大します。政府機関のIoTセキュリティ政策における国家レベルおよび国際レベルでの断片化は問題です。IoTソリューションは、本質的に相互に接続され、相互に依存しているためです。また、断片化された政策により、異なる市場で類似製品を販売するメーカーにとっては、市場に異なる要件や矛盾する要件が存在する可能性があるため販売が困難です。このような結果、競争力が低下し、技術革新が阻害され、ユーザーが最も安全なテクノロジーにアクセスすることができなくなります。

IoTセキュリティに対する政府のアプローチが確立されるにつれて、IoTデバイスやコンポーネントを開発する多国籍テクノロジー企業は、ポリシーガイダンス、規制要件、標準が複雑化していく状況に直面することになります。IoTソリューションのメーカーは、基盤となるコードがどこで開発されたか、デバイスがどこで製造されたかにかかわらず、世界中でデバイスを市場に投入したいと考えています。統一されておらず、一貫性がなく、矛盾する国家的、国際的な政策の状況により、これら企業は販売を疎外されることになり、その結果イノベーションと競争力が抑制されます。IoTセキュリティへのアプローチを調和させることは、グローバル経済にとって重要な目標です。

政府のIoTセキュリティ政策は、可能な限り、世界中で進行中の他の同様の取り組みの情報を取り入れ、これらに沿うよう調整する必要があります。

---

6 内務省の*Draft Code of Practice: Securing the Internet of Things for Consumers*、https://www.homeaffairs.gov.au/reports-and-pubs/files/code-of-practice.pdfを参照。

7 ENISA、*Good Practices for Security of Internet of Things in the Context of Smart Manufacturing*、https://www.enisa.europa.eu/publications/good-practices-for-security-of-iotを参照。また、ENISA 、*IoT Security Standards Gap Analysis*、https://www.enisa.europa.eu/publications/iot-security-standards-gap-analysisも合わせて参照。

8 経済産業省、*IoTセキュリティガイドライン*ver 1.0、https://www.meti.go.jp/english/press/2016/0705_01.htmlを参照。

9 *Infocomm Media Development Authority*、*Guidelines：Internet of Things（IoT）Cyber Security Guide*、https://www.imda.gov.sg/-/media/imda/files/regulation-licensing-and-consultations/consultations/open-for-public-comments/consultation-for-iot-cyber-security-guide/imda-iot-cyber-security-guide.pdfを参照。

10 デジタル・文化・メディア・スポーツ省、*Code of Practice for Consumer IoT Security*、https://www.gov.uk/government/publications/code-of-practice-for-consumer-iot-securityを参照。

11 SB-327　Information Privacy: Connected Devices（カリフォルニア州立法議会、2017–2018）、https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201720180SB327を参照。

12 Enrolled House Bill 2395（第80回オレゴン州立法議会、2019）、https://olis.leg.state.or.us/liz/2019R1/Downloads/MeasureDocument/HB2395/Enrolledを参照。.

IoTセキュリティ政策は、国際的に認められたIoT標準の開発と使用をサポートする

IoTテクノロジーには、国際的に認知されているいくつかの技術的なセキュリティ標準が適用できます。これらのセキュリティ標準は、効果的なセキュリティ方法を定義して実装するための、広く検討された合意に基づく情報とガイダンスを提供し、共通の課題に対する一般的なアプローチを促進して、協働性と相互運用性を実現します。IoT標準は、さまざまなユースケース展開、ベンダー、セクター、地域にわたる相互運用性を促進し、IoTの長期的な実行可能性を維持し、IoTソリューションのメリットとセキュリティの公平な分配を促進します。相互運用性の向上と、オープンで自発的、広く利用可能な標準をIoTデバイスの技術的な構成要素として採用することで、ユーザーのメリット、革新性、経済的な機会が拡大します。[13]IoTに関する規制、認証、その他の政府の政策は、どこに帰属するものであっても、合意に基づき、国際的に認知されたセキュリティ標準に基づいている必要があります。IoT標準がまだ存在しない場合、政策立案者はIoTへの技術的なアプローチを義務化しないようにし、業界、研究者、その他の関係者が相互運用性へのサポートを目的としてオープンで合意に基づく標準の開発に協力するように奨励する必要があります。これは、既存の標準化開発委員会をサポートし、M2Mの相互運用性など、進化していく標準が必要となる分野についての学術研究に資金を提供することで実現できます。

政府のIoTセキュリティ政策は、それが存在する場所にかかわらず、世界的、自発的、そして合意に基づく基準と一致したものでなければならず、国際的に認知された新しいIoTセキュリティ標準の開発をサポートし、国際的なベストプラクティスとは異なるローカライズされた標準や認証は控える必要があります。

IoTセキュリティ政策は、必要に応じて適切にベースラインセキュリティ要件を設定する

政府がIoTセキュリティ政策を策定する際には、IoTエコシステムの複雑さとコンシューマー向けIoTとIIoTの違いを考慮して、一部の分野でIoTセキュリティ規制が必要であると政策立案者は判断するかもしれません。これらの特定の状況では、セキュリティガイダンスでコアセキュリティ機能を特定することが必要です。コアIoTセキュリティ機能は、サイバーセキュリティに関連するアクティビティで構成されており、メーカーが該当するすべてのIoT製品で対処することを推奨します。これらの活動により、メーカーはIoTデバイスの顧客に対するサイバーセキュリティの負担を軽減できます。これにより、IoTデバイスのセキュリティ侵害や、セキュリティ侵害のあるIoTデバイスを使用して行われる攻撃の発生率と深刻度を低減できます。

セキュリティ機能は、IoTデバイスの製造、導入、使用、所有権の移転、終了、最終的な廃棄など、IoTデバイスが使用可能なライフサイクル全体に対応する必要があります。したがって、使用可能なライフサイクル全体で、必然的に異なる関係者と責任当事者が存在します。

状況に応じて、IoTのコアセキュリティ機能の政策立案者は、暗号化、パッチ適用性、ID管理、信頼の基点（RoT）、セキュアな開発ライフサイクル（SDLC）などを検討できます。このような基本的な要件は、常に国際的に認められた基準と一致し、技術開発に十分に対応できる柔軟性を維持する必要があります。

---

[13] 国際標準に準拠することで、政府のセキュリティに関する取り組みや政策の広範な採用を促進できます。たとえば、国立技術標準研究所の*Framework for Improving Critical Infrastructure Cybersecurity*（重要インフラのサイバーセキュリティを改善するためのフレームワーク）は、国際的に認められた基準に沿っており、4か国語での翻訳と国際政府5機関による適応が示すように、世界中で使用されています。詳細については、NIST、International Perspectives、https://www.nist.gov/cyberframework/international-perspectivesを参照。また、NIST、International Resources、https://www.nist.gov/cyberframework/international-resourcesも合わせて参照。

» **暗号化:**IoTテクノロジーは、デバイスの導入方法や、その使用に伴うプライバシーやセキュリティのリスクに応じて、暗号化するデータと使用する暗号化メカニズムを定義する暗号化戦略に従って開発する必要があります。

» **パッチ適用性:**特に、管理されたセキュリティ環境での使用が想定されないコンシューマー向けIoT製品の場合、IoTテクノロジーは、遠隔または直接に、安全な更新プログラムとセキュリティパッチを受信できる必要があります。

» **アイデンティティ管理:**機密情報を処理したり、アクセスを制御するIoTテクノロジーは、パスワードやその他のユーザー認証情報に最新の業界ベストプラクティスを適用するなど、強力なID管理と認証を提供する必要があります。

» **信頼の基点(RoT):**IoTテクノロジーでは、より強固なセキュリティ保証を実現するために、RoTにおいて適切にセキュリティメカニズムの基盤を置く必要があります。RoTは、特定の重要なセキュリティ機能を実行する、信頼性の高いハードウェア、ファームウェア、およびソフトウェアコンポーネントです。RoTは本質的に信頼性を有するものなので、設計上安全である必要があります。そのため、RoTの多くはハードウェアには実装されています。提供する機能がマルウェアによって改ざんされることがないようにするためです。RoTは、セキュリティと信頼を構築するための強固な基盤を提供します。

» **セキュアな開発ライフサイクル:**BSA会員企業は、SDLCの概念を作り上げる業界リーダーであり続けてきました。製品開発段階のセキュリティに関して考慮すべき事項の重視や、製品のライフサイクル全体にわたるセキュリティ問題の管理、また、脆弱性や欠陥が発見されたときの分析に基づいて開発プロセスを改善するための反復学習も行います。セキュアな開発ベストプラクティスを採用し、サプライチェーンのリスクを管理し、特定された脆弱性を緩和し、エンドオブライフにおける考慮事項に対処するというベンダーのコミットメントを含むSDLCは、IoTデバイスのハードウェア、ファームウェア、およびソフトウェア要素にとって不可欠です。「BSA Framework for Secure Software」では、ソフトウェアのSDLC要素に関するガイダンスを提供しています。

政策立案者がリスクを判断する際に必要となるIoTセキュリティ政策には、特定のセキュリティ要件、暗号化、パッチ適用性、アイデンティティ管理、RoT、セキュアな開発ライフサイクルなどのコアセキュリティ機能が含まれ、広く受け入れられている国際標準に準拠する必要があります。これら国際標準は、最新のテクノロジーとセキュリティプラクティスに対応するべく定期的に更新されています。

セキュリティ機能は、IoTデバイスの製造、導入、使用、所有権の移転、終了、最終的な廃棄など、IoTデバイスが使用可能なライフサイクル全体に対応する必要があります。

プライバシーとIoT

IoTデータの保護は、セキュリティとプライバシーの両方のリスクを軽減するために不可欠です。IoTデバイスが世界中で市場を拡大するにつれ、消費者がデータを有意義に制御できることがますます重要になってきます。データプライバシーのベストプラクティスは、セキュリティに関わる手続きを強化することができ、収集されたデータの機密性とその使用目的の両方を反映させながら、IoT環境に順応させるべきです。これらの原則はIoTセキュリティに重点を置いていますが、IoTテクノロジーを使用する際には、消費者のプライバシーを保護するための補完的なアプローチを検討する必要があります。IoTアプリケーションによって収集されたデータも含む、データプライバシーに対する包括的なアプローチは、テクノロジーが消費者のプライバシーを保護するのに役立ちます。

IoTセキュリティ政策は、セキュリティをIoTの取得に統合する

今後、コンシューマー向けまた産業向けのIoTテクノロジーが普及するにつれ、IoTソリューションの政府による利用も増加すると予想されます。調達ガイドラインの策定や、情報に基づくリスクベースの分析によるサプライチェーンリスク測定のためのポリシーの設定において、政府機関は民間のサイバーセキュリティに積極的に影響を与えることができます。同様に、IoT調達においてセキュリティを優先することは、幅広いIoT市場により安全な製品の製造を奨励することになるので、消費者に利益をもたらします。

IoTデバイス、プラットフォーム、サービスの調達方法の強化を検討している政策立案者は、国際的に認められ適用可能な標準と政策が一致していることを確認し、セキュリティのベストプラクティスに準拠していることを強調する必要があります。そのため、多層化されたハードウェアおよびソフトウェアレベルの機能を備えたセキュアなソリューションは、政府のIoTの調達の優先事項となります。

政府は、調達プロセスの部門や機関を奨励し、業界主導の、自発的な、合意に基づく国際ガイドラインに基づいて、安全で相互運用性が高く、拡張性に優れた資産向けIoTソリューションを優先する必要があります。

IoTセキュリティ政策は、IoTをインシデント対応に組み込む

IoTアプリケーションが急増し、消費者や産業界のユーザーにメリットがもたらされる中、政府はIoTをインシデント時や緊急時の対応に組み込むべきです。IoT攻撃は複雑で動的であり、サイバー脅威や物理的な脅威を伴う可能性があるため、大規模なIoTインシデントへの対応や解決は特に困難です。政策立案者は、IoTに関する考慮事項をインシデント対応計画および政策の作成に組み込むべきです。これにより、IoT攻撃の潜在的なスピードと規模に対応できます。さらに、政策立案者は、IoTテクノロジーがどのようにして緊急計画と対応を改善できるかを検討する必要があります。これには、業務上必須なロジスティクスのサポートと通信、緊急通報、公共警報システムなどが含まれます。

政府は、IoTをインシデント対応計画に統合すべきです。これには、IoTのインシデントや緊急対応の政策とプログラムが含まれます。

IoTテクノロジーは、私たちの日常生活とビジネスプロセスを急速に変化させています。IoTソリューションの普及に伴い、IoTエコシステム全体のセキュリティを促進するためには、政策立案者が迅速に行動する必要があります。サイバーセキュリティとIoTイノベーションのリーダーを代表して、BSAは、IoTセキュリティに対する責任あるリスクベースのアプローチを強く支持します。
上記の原則は、政府がこの複雑な政策課題に取り組む際の指針となります。BSAは、IoT市場全体のセキュリティを推進するために、政策立案者と協力する機会を歓迎します。

主なリソース

BSA | ザ・ソフトウェア・アライアンス、*The BSA Framework for Secure Software*、2019 年4月29日。https://www.bsa.org/reports/bsa-framework-for-secure-software

Charter of Trust、*Charter of Trust Principles*、https://www.charteroftrust.com/wp-content/uploads/2020/02/200212_Dok-Narrative_A4_EN_200212.pdf

シスコ、*Cisco Annual Internet Report (2018–2023)*、2020年3月。https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.pdf

Council to Secure the Digital Economy、*The C2 Consensus on IoT Security Baseline Capabilities*、2019年9月17日。https://securingdigitaleconomy.org/projects/c2-consensus/

国防総省、*DoD Policy Recommendations for the Internet of Things (IoT)*、2016年12月。https://www.hsdl.org/?view&did=799676

European Telecommunications Standards Institute（欧州電気通信規格協会）、*EMTEL; Study of use cases and communications involving IoT devices in provision of emergency situations*、2019年7月。https://www.etsi.org/deliver/etsi_tr/103500_103599/103582/01.01.01_60/tr_103582v010101p.pdf

European Union Agency for Cybersecurity（欧州ネットワーク・情報セキュリティ機関）、*Good Practices for Security of Internet of Things in the context of Smart Manufacturing*、2018年11月29日。https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot

インテル、Internet of Things Policy Framework、https://www.intel.com/content/www/us/en/policy/policy-iot-framework.html

国際標準化機構、*情報技術—クラウドコンピューティング—概要および用語*、ISO/IEC 17788（2014）。

国際標準化機構、*情報技術—クラウドコンピューティング—エッジコンピューティングランドスケープ*、ISO/IEC 23188（2020）。

国際標準化機構、*情報技術—モノのインターネット（IoT）—用語*、ISO/IEC 20924（2019）。

国際標準化機構、*情報技術—セキュリティ技術—アプリケーションセキュリティ、パート1－7*、ISO/IEC 27034（1：2011 - 7：2018）。

国際標準化機構、*情報技術—セキュリティ技術—脆弱性開示*、ISO/IEC 29147（2019）。

国際標準化機構、*情報技術—セキュリティ技術—脆弱性処理プロセス*、ISO/IEC 30111（2019）。

国際標準化機構、*モノのインターネット（IoT）—IoTシステムの相互運用性ーパート1：フレームワーク*、ISO/IEC 21823-1（2019）。

国際標準化機構、*モノのインターネット（IoT）—リファレンス・アーキテクチャ*、ISO/IEC 30141（2018）。

マイクロソフト、*Cybersecurity policy for the Internet of Things*、https://www.microsoft.com/en-us/cybersecurity/content-hub/iot-cybersecurity-policy

マイクロソフト・リサーチNExTオペレーティングシステムテクノロジーグループ、*The Seven Properties of Highly Secure Devices*、2017年3月。https://www.microsoft.com/en-us/research/wp-content/uploads/2017/03/SevenPropertiesofHighlySecureDevices.pdf

National Institute of Standards and Technology(米国標準技術局)、NISTIR 8259、*Foundational Cybersecurity Activities for IoT Device Manufacturers*、2020年5月29日。https://www.nist.gov/publications/foundational-cybersecurity-activities-iot-device-manufacturers

National Institute of Standards and Technology(米国標準技術局)、NISTIR 8259A、*IoT Device Cybersecurity Capability Core Baseline*、2020年5月29日。https://www.nist.gov/publications/iot-device-cybersecurity-capability-core-baseline

PTC、*The State of Industrial Internet of Things 2019:Spotlight on Operational Effectiveness*(2019年)。https://www.ptc.com/-/media/Files/PDFs/IoT/State-of-IIoT-Report-2019.pdf